UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/658,387	09/08/2000	Aureliano Tan JR.	05452.002002	3461

22511 7590 05/25/2007

OSHA LIANG L.L.P.
1221 MCKINNEY STREET
SUITE 2800
HOUSTON, TX 77010

EXAMINER	
KLIMACH, PAULA W	
ART UNIT	**PAPER NUMBER**
2135	

MAIL DATE	DELIVERY MODE
05/25/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/658,387	TAN, AURELIANO	
	Examiner	Art Unit	
	Paula W. Klimach	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 March 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,6,8,9,34,64,69 and 72-75* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 6, 8-9, 34, 64, 69, and 72-75* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 03/01/07. The amendment filed on 03/01/07 have been entered and made of record. Therefore, presently pending claims are 1, 6, 8-9, 34, 64, 69, and 72-75.

Response to Arguments

Applicant's arguments filed 03/01/07 have been fully considered but they are not persuasive because of following reasons.

Applicant argued that Jones and Gammie are completely silent with respect to any embodiment in which user is the owner. The new reference discloses the information as the owner's, the person purchasing the software, information.

The applicant argued further that Jones is the password of Jones is not equivalent to a name of an owner of the digital identity device. The new reference, Cooper, teaches this limitation as shown in the rejection below.

The applicant argues further that the references in the previous office action did not teach microprocessor identity comprising an alpha-numeric value. The new reference, Cooper, teaches this limitation as shown in the rejection below.

In reference to claims 69 and 72 the applicant does not see how a digital signature generated by the manufacturer could be construed to be any way equivalent to any of the pieces of information listed. However in the rejection of claims 69 and 72, the reference Friedman teaches a method securing a digital image. The image is of a corporate officer and therefore

corresponds to the name of a corporate officer since it shows a facial image which is associated with a name.

In reference to claim 73 Jones teaches and two separate memories; (i) a digital identity device including two separate memories; (ii) digital identity data stored in the first memory; and (iii) an operating system in the second memory binding the digital identity data and the microprocessor identity (Fig. 3).

Dependent Claims are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 6, 8-9, 69-72 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones (5623637) in view of Cooper (5,689,560) and further in view of the article by Friedman ("The Trustworthy Digital Camera: Restoring Credibility To The Photographic Image").

In reference to claim 1. Jones discloses a system for storing a password value and logic circuitry for preventing access to information stored on the memory card unless the user of the host computer to which the memory card is connected can supply a password matching the stored password (abstract). Jones also discloses a microprocessor (Fig. 1 part 260). Jones discloses further digital identity data (password part 301 Fig. 2), wherein the digital identity data

uniquely identifies a user of the digital identity device. The password is digital data that uniquely identifies a user because only the user would know the password (column 3 lines 39-43 in combination with column 8 lines 35-41). The system of Jones contains a memory configured to store at least the digital identity data (column 7 lines 32-41). The system of Jones discloses digital identity data that is encrypted by the digital identity data using an algorithm that uses a random number (column 8 lines 4-34)

Although Jones discloses a microprocessor (Fig. 1 part 260) and the encryption of the user data, Jones does not discloses a microprocessor wherein the identity is stored in the microprocessor.

Cooper discloses a method and apparatus is provided for distributing software objects from a producer to a potential user (abstract). The system discloses the encryption of personal information (key file) using serial number (key; column 15 line 62 to column 16 line 9). Cooper further discloses a digital identity that comprises a name of the owner (column 13 lines 10-17), wherein the microprocessor identity is an alpha-numeric value (column 13 line 65 to column 14 line 5).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the security program as in Cooper in the system of Jones. One of ordinary skill in the art would have been motivated to do this because it would discourage the unauthorized use of data Cooper column 2 lines 12-25).

Although Jones discloses a microprocessor and the encryption of the user data, and Cooper disclose the encryption of user data with a key derived from a machine id, neither Jones nor Cooper disclose the storage of the machine id in the microprocessor.

Friedman discloses a method securing a digital image (abstract). The image is secured using a unique key, therefore identification, which is etched to the camera's secure microcontroller (page 908 column 2, the first full paragraph).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to etch the key into the controller as performed by Friedman in the system of Jones. One of ordinary skill in the art would have been motivated to do this because credibility of the camera's output becomes an extension of that of the manufacturer; thus a digital signature from the camera can be considered to be just as reliable and secure as if the signature had been generated by the manufacturer (Friedman page 908 column 1, the first full paragraph).

In reference to claim 6, wherein the digital identity is for one of the group consisting of an individual and a corporation; and wherein the digital identity at least one selected from the group consisting of a digital picture, an address, a date of birth, a social security number, a driver's license number, a digital photograph, biometric information, credit card information, and a database administrator name (business data, column 1 lines 15-25).

In reference to claim 8, wherein the digital identity device further comprises a computer an interface configured to enable the digital identity device to communicate with an external device (Fig. 1).

In reference to claim 9, wherein the interface comprises an input/output port (column 5 lines 50-55).

In reference to claims 69 and 72 wherein the owner is a corporation, wherein the name is an incorporation name of the corporation, and wherein the digital identity data comprises at least

one selected from the group consisting of a data and place of incorporation of the corporation, a name of a corporate officer of the corporation, and corporate partner of the corporation.

Friedman discloses a method securing a digital image (abstract). The image is secured using a unique key, therefore identification, which is etched to the camera's secure microcontroller (page 908 column 2, the first full paragraph).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to etch the key into the controller as performed by Friedman in the system of Jones. One of ordinary skill in the art would have been motivated to do this because credibility of the camera's output becomes an extension of that of the manufacturer; thus a digital signature from the camera can be considered to be just as reliable and secure as if the signature had been generated by the manufacturer (Friedman page 908 column 1, the first full paragraph).

Claims 34, 64, and 73-75 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones (5623637) in view of Cooper and further in view of Friedman as in claim 1 and further in view of Guthery and Yap et al (6,111,506) and further in view of Paolini (6,847,948).

In reference to claims 34 and 73, is rejected as disclosed in claim 1 above. In reference to claim 73; Jones teaches and two separate memories; (i) a digital identity device including two separate memories; (ii) digital identity data stored in the first memory; and (iii) an operating system in the second memory binding the digital identity data and the microprocessor identity (Fig. 3). The additional limitation of obtaining digital identity data form a digital device operatively connected to a computer in which the electronic document is stored is taught by Guthery.

Guthery discloses a computer having a microprocessor containing identity information (column 5 lines 25-40 in combination with column 6 line 49 to column 7 line 5). The system includes obtaining digital identity data from a digital identity device operatively connected to a computer in which the electronic document is stored (Fig. 1). Guthery discloses a system that comprises a microprocessor (Fig. 2 part 52). Guthery further disclose a system that comprises digital identity data wherein the digital identity data is associated with a user of the digital identity device; a memory configured to store at least the digital identity data (column 5 lines 7-15; column 6 lines 44-50; column 7 lines 13-21; Fig 2 part 58).

Guthery discloses a card ID (column 7 lines 1-5) which posses as the microprocessor identity due to the fact that the card ID belongs to the card; and therefore everything on the card and the card only has one microprocessor (Fig. 2). It follows that the ID identifies the contents of the card and therefore identifies the microprocessor. Even if the card ID is not a microprocessor identity, Paolini discloses a method and apparatus is disclosed for preventing an unauthorized computer system form using copied software of data (abstract). The system uses a CPU ID (microprocessor ID) of a particular computer system (column 3 lines 1-5).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a microprocessor ID in the smart card of Paolini in the system of Guthery. One of ordinary skill in the art would have been motivated to do this because the ID is a unique quantity that can be used to prevent the use of copied software.

Although Guthery discloses storing information such as licenses and therefore documents (column 6 lines 45-50) and the system has passwords (column 6 lines 62-67) and a program for encryption (column 6 lines 25-30), Guthery does not disclose encrypting the documents

Yap discloses storing documents on the smart card. The documents are encrypted.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to encrypt the documents as in Yap with the digital identity data of Guthery and storing the documents on the smart card as in Guthery. One of ordinary skill in the art would have been motivated to do this because it would discourage fougery.

Guthery and Paolini do not disclose the etching of the microprocessor identity information into the microprocessor

Friedman discloses a method securing a digital image (abstract). The image is secured using a unique key, therefore identification, which is etched to the camera's secure microcontroller (page 908 column 2, the first full paragraph).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to etch the key into the controller as performed by Friedman in the system of Jones. One of ordinary skill in the art would have been motivated to do this because credibility of the camera's output becomes an extension of that of the manufacturer; thus a digital signature from the camera can be considered to be just as reliable and secure as if the signature had been generated by the manufacturer. (Friedman page 908 column 1, the first full paragraph).

In reference to claims 64 and 74, wherein the digital identity is for one of the group consisting of an individual and a corporation; and wherein the digital identity at least one selected from the group consisting of a digital picture, an address, a date of birth, a social security number, a driver's license number, a digital photograph, biometric information, credit card information, and a database administrator name (bank information, column 7 lines 45-47; and column 6 lines 47).

In reference to claim 75 wherein the owner is a corporation, wherein the name is an incorporation name of the corporation, and wherein the digital identity data further comprises at least one selected from the group consisting of an incorporation name of the corporation, a data and place of incorporation of the corporation, a name of a corporate officer of the corporation, and corporate partner of the corporation.

Friedman discloses a method securing a digital image (abstract). The image is secured using a unique key, therefore identification, which is etched to the camera's secure microcontroller (page 908 column 2, the first full paragraph).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to etch the key into the controller as performed by Friedman in the system of Jones. One of ordinary skill in the art would have been motivated to do this because credibility of the camera's output becomes an extension of that of the manufacturer; thus a digital signature from the camera can be considered to be just as reliable and secure as if the signature had been generated by the manufacturer (Friedman page 908 column 1, the first full paragraph).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-38544. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Thursday, May 24, 2007

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100